

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.</small>					
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 02-05-2013		2. REPORT TYPE Master of Military Studies Research Paper		3. DATES COVERED (From - To) September 2012 - May 2013	
4. TITLE AND SUBTITLE The MAGTF's Reliance On The Global Positioning System: A Critical Vulnerability				5a. CONTRACT NUMBER N/A	
				5b. GRANT NUMBER N/A	
				5c. PROGRAM ELEMENT NUMBER N/A	
6. AUTHOR(S) Browne, Desmond F., Major, USMC				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER N/A	
				5f. WORK UNIT NUMBER N/A	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068				8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				10. SPONSOR/MONITOR'S ACRONYM(S) N/A	
				11. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A	
12. DISTRIBUTION AVAILABILITY STATEMENT Unlimited					
13. SUPPLEMENTARY NOTES N/A					
14. ABSTRACT The overarching goal of this research study is to gain a greater understanding of the effects and implications that anti-GPS threats can have on the employment of GPS within the MATGF given the context of a plausible, real-world scenario. The study begins by providing an overview of key concepts relevant to the problem and examines current and emerging threats within the contemporary environment. The study then conducts a qualitative assessment of the impact Anti-GPS threats can have on a MAGTF's capabilities using several plausible vignettes. It examines and assesses potential rival claims and opposing viewpoints in relation to the study's assessment. Finally, the study provides recommendations regarding future GPS use within the MAGTF.					
15. SUBJECT TERMS GPS; A2AD; MAGTF; Anti-Access; Critical Vulnerability					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 63	19a. NAME OF RESPONSIBLE PERSON Marine Corps University / Command and Staff College
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPHONE NUMBER (Include area code) (703) 784-3330 (Admin Office)

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

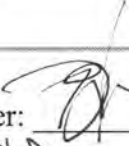
MASTER OF MILITARY STUDIES

**THE MAGTF'S RELIANCE ON THE GLOBAL POSITIONING SYSTEM:
A CRITICAL VULNERABILITY**

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

MAJOR DESMOND F. BROWNE JR., USMC

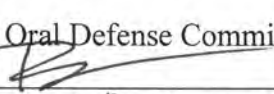
AY 12-13

Mentor and Oral Defense Committee Member: 

Approved: Benjamin Jensen, PhD

Date: 8 April 13

Mentor and Oral Defense Committee Member: Rebecca J. Johnson

Approved: 

Date: 8 April 2013

Mentor and Oral Defense Committee Member: _____

Approved: _____

Date: _____

Table of Contents

	Page
DISCLAIMER	i
EXECUTIVE SUMMARY	ii
PREFACE	iv
INTRODUCTION	1
KEY CONCEPTS	3
THE THREAT ENVIRONMENT	11
QUALITATIVE ASSESSMENT	20
COUNTERARGUMENTS	30
RECOMMENDATIONS	44
CONCLUSION	46
NOTES	47
BIBLIOGRAPHY	55

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEW OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FORGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Executive Summary

Title: The MAGTF's Reliance on the Global Positioning System: A Critical Vulnerability

Author: Major Desmond F. Browne Jr., United States Marine Corps

Thesis: The Marine Corps, as an institution, does not recognize the extent to which GPS is vulnerable, the potential effects of many Anti-GPS threats, and the extent to which the Marine Corps has become over-reliant on GPS to conduct critical activities in support of operations. Therefore, if GPS or clusters of GPS enabled systems are disrupted or disabled, then a MAGTF's ability to conduct operations during crises or contingencies will be jeopardized.

Discussion: The expanded application and integration of GPS technology into systems, munitions, and equipment has markedly improved the operational capability of the MAGTF. However, the Marine Corps' increasing reliance on GPS technology has not gone unnoticed by competitor nations and our adversaries. They are actively pursuing new and more highly capable Anti Access and Area Denial (A2/AD) systems and weapons. Perhaps the most dangerous and rapidly evolving A2/AD threat comes from Anti-GPS capabilities. Anti-GPS capabilities attack the control, space, or user segments comprising GPS in order to disrupt, deny, neutralize, or destroy their functionality. The threats from GPS jamming, spoofing, cyber warfare, and kinetic attack provide new ways for potential adversaries to undermine a MAGTF's operational capability with scalable effects. Anti-GPS capabilities can be applied at all levels of warfare on the spectrum of conflict and they can be utilized by nation states, organizations, and non-state actors. Although the effects from Anti-GPS threats vary, the impact on a MAGTF's operational capability is likely to be severe. Furthermore, the contemporary MAGTF is ill equipped defend against the full range of Anti-GPS threats.

Conclusion: To mitigate the effects of Anti-GPS capabilities, this study offers three recommendations. First, the Marine Corps should ensure diversity in its systems and avoid

developing capabilities that are entirely reliant on GPS. Second, the Marine Corps should ensure proficiency with training standards that require the use of non-GPS methods to accomplish critical tasks. Third, the Marine Corps Warfighting Lab (MCWL) should conduct testing / evaluation to gather additional qualitative and quantitative data regarding the effects of Anti-GPS threats on a MAGTF's operational capabilities.

Preface

My interest in studying the ability of a Marine Air Ground Task Force (MAGTF) to operate in a GPS disrupted / denied environment comes as a result of the Marine Corps increasing reliance on GPS technology to plan, coordinate, and fight. In recent years, advances in technology combined with the increasing requirement for precision and speed has expanded the application of GPS technologies. As a result, many of the tasks and activities performed throughout a MAGTF now integrate GPS or are enabled by GPS to some extent. However, the increasing use and integration of GPS is problematic due to the wide array of Anti-GPS capabilities which can threaten both the employment of GPS and the ability of a MAGTF to carry out critical tasks. In my judgment, this possibility presents a critical issue that has not received adequate consideration within the Marine Corps. Therefore this study will examine this issue in order to help shape the way in which the Marine Corps employs GPS technology, trains, and fights in the future.

In completing this research and writing this paper, I wish to acknowledge the support of my Marine Corps University mentor Dr. Benjamin Jensen. Throughout this process, he has provided the motivation, guidance, and constructive ideas which have tremendously aided my efforts and the development of this research study. In addition, I wish to thank my wife Stephanie, who provided patience and support throughout the long hours of research and writing to complete this study.

Introduction

The Global Positioning System (GPS) became fully operational in 1995 as a way to enable precision navigation for the United States military.¹ Today, GPS enhances the ability of a Marine Air Ground Task Force (MAGTF) to not only navigate, but also to conduct targeting, deliver fires, and synchronize radio communications. The expanded application and integration of GPS technology into systems, munitions, and equipment has markedly improved the capability of MAGTF operations in the contemporary environment. The advantages created through GPS technology include but are not limited to precision fires, increased operational tempo, greater situational awareness, an enhanced ability to coordinate, and reduced risk to operations. Given the many advantages GPS provides, one can reasonably assert that GPS will continue to be a critical capability for MAGTF operations in the future. However, the Marine Corps' increasing reliance on GPS technology has not gone unnoticed by competitor nations such as Russia and China, and potential adversaries such as North Korea and Iran. These nations and many others are actively pursuing new and more highly capable Anti Access and Area Denial (A2/AD) systems and weapons.

The term, A2/AD refers to threat capabilities that can be employed by an adversary to deter or counter U.S. forces from deploying to, or operating within, a defined space.² In general, A2/AD threats encompass a wide range of capabilities to include cyber warfare, space capabilities, cruise and ballistic missiles, and mine warfare.³ Arguably, one of the most dangerous and rapidly evolving A2/AD threats to emerge within the last 20 years is from Anti-GPS capabilities. A variety of Anti-GPS capabilities such as GPS jammers, cyber warfare, and anti-satellite weapons, provide new ways for potential adversaries to undermine a MAGTF's operational capability with scalable effects.

While the effectiveness of many Anti-GPS capabilities remains contested, it is reasonable to assert that current and emerging threats will be capable of disrupting or denying the ability of a MAGTF to employ GPS under a variety of conditions. Therefore, Anti-GPS capabilities will increasingly present a formidable challenge to MAGTF operations. However, a central question that remains to be answered is, to what extent would MAGTF capabilities be affected by Anti-GPS threats? Although more lethal A2AD capabilities exist, the Anti-GPS threat is a critical issue because the Marine Corps does not recognize the extent to which GPS is vulnerable, the potential effects of most Anti-GPS threats, and the extent to which the Marine Corps has become over-reliant on GPS to conduct critical activities in support of operations. Therefore, if GPS or clusters of GPS enabled systems are disrupted or disabled, then a MAGTF's ability to conduct operations during crises or contingencies will be jeopardized.

The overarching goal of this research study is to gain a greater understanding of the effects and implications that anti-GPS threats can have on the employment of GPS within the MAGTF given the context of a plausible, real-world scenario. To provide a complete examination of the issues pertaining to the problem, this research study will utilize the following framework. The study will begin by providing an overview of key concepts relevant to the problem and examine current and emerging threats within the contemporary environment. The study will then conduct a qualitative assessment of the impact Anti-GPS threats can have on a MAGTF's capabilities using several plausible vignettes. It will examine and assess rival claims and opposing viewpoints in relation to the study's assessment. Finally, the study will provide recommendations regarding future GPS use within the MAGTF.

Underpinning this approach are four key assumptions. First, GPS technology will remain a critical capability for the Marine Corps and its integration into operations will continue to

expand. Second, Marine Corps organizational culture generally does not appreciate the full extent to which GPS enables critical activities across the Warfighting Functions. Third, Anti-GPS threats will continue to develop and improve in reaction to U.S. efforts to safeguard GPS enabled technology (action/reaction/counteraction cycle). The final assumption is Marine Corps organizational culture generally does not understand the vulnerabilities existing and inherent with the current GPS structure and functionality. These assumptions are relative to this study's thesis because arguably, they describe the conditions under which the Marine Corps is currently operating. In effect, the Marine Corps is linking a critical enabler of a MAGTF's operational capability to a system (GPS) that is both recognized as vulnerable by potential adversary's but not sufficiently safeguarded.

In order to prove that A2/AD threats can jeopardize a MAGTF's operational capability, the study must demonstrate GPS or clusters of GPS enabled systems across one or more Warfighting functions can be degraded or disabled. In doing so, the research study will increase institutional awareness and induce ideas or concepts to mitigate the effects of Anti-GPS threats on the MAGTF. However, if the study is unable to validate that a MAGTF's capabilities are jeopardized by A2/AD threats, the results should demonstrate that either sufficient countermeasures exist to defeat Anti-GPS technology, or activities conducted within the MAGTF are capable of sustaining effective operations regardless of A2/AD threats. Such a conclusion would validate the design and capability of GPS technologies and the approach to utilize GPS within the Marine Corps.

Key Concepts

The foremost concept to explain from the outset of this research study concerns GPS itself. To inform the study about GPS, two central questions will be addressed in detail: first,

what is GPS, and second, how does GPS work? In answering these questions the study will establish the basis for analyzing how GPS is vulnerable, how GPS can be attacked, and how it should be protected. Moreover, this understanding (of GPS) will provide greater context for the vignettes, inferences, and recommendations later in the study. The first aspect of this concept to explain is, what GPS is.

What is GPS?

GPS is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) service.⁴ GPS is comprised of three components referred to as segments: the space segment, the control segment, and the user segment.⁵ The U.S. Air Force develops, maintains, and operates the space and control segments to provide the user segment with PNT service.⁶ The user segment is generally regarded as the military or civilian user/organization operating a GPS receiver. There are an unlimited number of GPS users and various types of GPS receivers throughout the user segment. However, the intricacy of the three GPS segments requires each to be examined in further detail. Arguably the most complex, yet critical segment of GPS is the space segment.

Space Segment

The space segment is perhaps the most important segment of GPS; however, it also presents the most difficult segment for an adversary to attack. The space segment consists of a constellation of 31 operational satellites of varying age and capability that orbit earth twice a day at an altitude of 20,200 kilometers.⁷ The satellites provide reliable service over a 7.5- to 11-year design life while requiring minimal interaction with the control segment.⁸ As depicted in Figure 1, satellites in the constellation are arranged into six equally-spaced orbital planes, each containing a minimum of four "slots" occupied by GPS satellites.⁹ The arrangement of satellites

ensures there are at least four satellites in view from virtually any point on earth to allow for optimal reception of PNT service.¹⁰ Although extremely robust by design, the space segment is not entirely autonomous and relies on the control segment for effective command and control, and system maintenance functions.

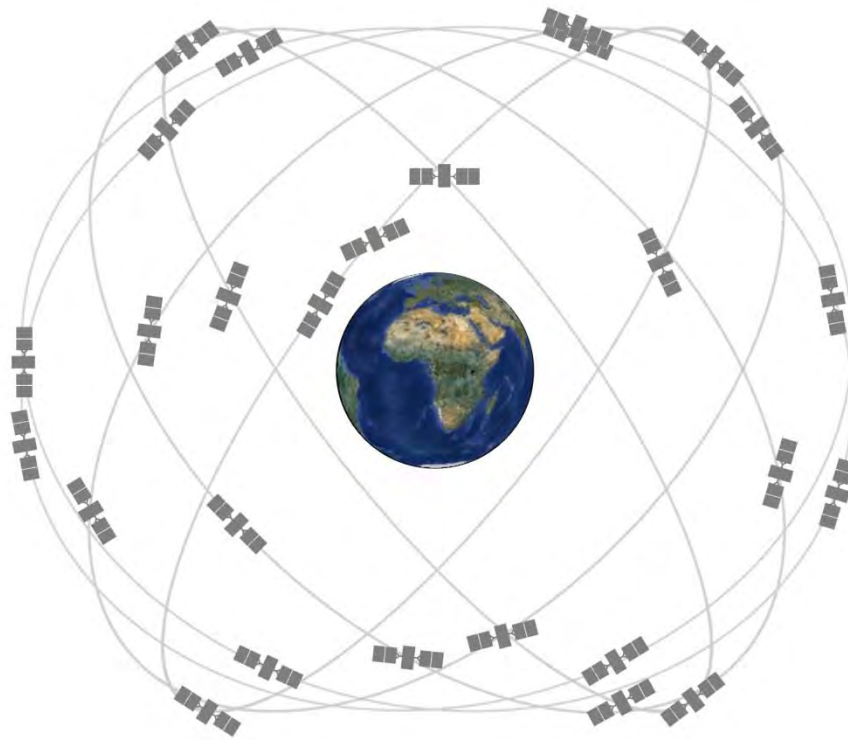


Figure 1. GPS Space Segment¹¹

Source: GPS.GOV, NOAA, <http://www.gps.gov/systems/gps/space/>

Control Segment

The control segment is arguably the second most important and second most difficult segment of GPS to attack. The control segment, is comprised of four components as shown in Figure 2: a Master Control Station (MCS), an Alternate Master Control Station (AMCS), twelve command and control ground antennas (GAs), and a network of sixteen globally-distributed monitor stations (MSs).^{12,13} The MCS, located at Schriever Air Force Base, Colorado, is the central control node for the GPS satellite constellation and it maintains continuous command and

control of the GPS constellation.¹⁴ The major tasks of the MCS include: (1) satellite monitoring (2) satellite maintenance and anomaly resolution (3) monitoring and management of GPS signal standards (4) NAV message transmissions to satellites and (5) detecting and responding to GPS failures.¹⁵ The control segment works to ensure uninterrupted services are provided to the third and final segment of GPS, the user segment.

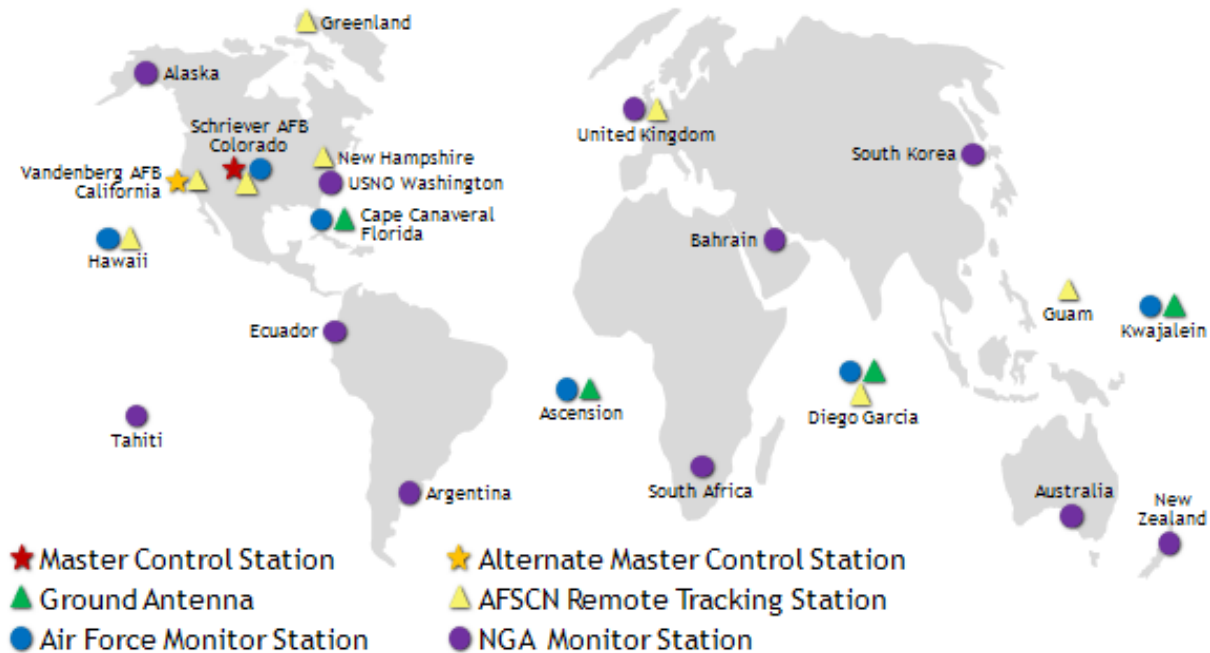


Figure 2. GPS Control Segment¹⁶

Source: GPS.GOV, NOAA, <http://www.gps.gov/systems/gps/control/>

User Segment

The user segment is arguably the least difficult segment of GPS to attack with Anti-GPS capabilities. The User Segment is large and diverse. It is comprised of civil and military users, inside and outside the United States. GPS supports both the individual user and large scale commercial industries. As Figures 3 and 4 convey, the Civil and Military applications for GPS span across a wide variety of critical activities.¹⁷ For the military, the range of critical activities supported by GPS spans across the warfighting functions of fires, maneuver, command and

control, intelligence, logistics, and force protection. However, every supported activity within the user segment, whether it is critical or not, relies on the successful interface between the three segments of GPS. To understand the functionality of GPS, and to further establish the basis for examining the vulnerability and threats against GPS, this study will take up the question of how GPS works.

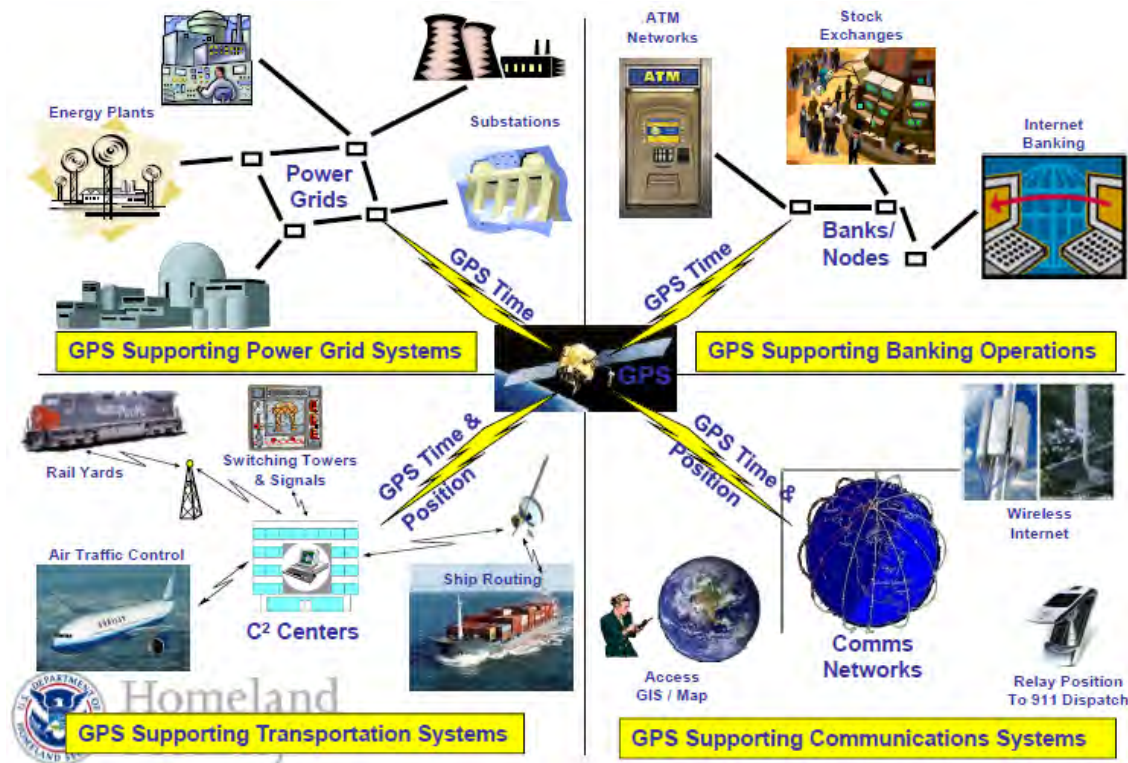


Figure 3. User Segment, Civil Use¹⁸

Source: John Merrill, "Patriot Watch VIGILANCE SAFEGUARDING AMERICA"
www.gps.gov/multimedia/presentations/2012/03/WSTS/merrill.pdf



Figure 4. User Segment, Military Use

How does GPS work?

GPS functions through a combination of interfaces between the Control, Space, and User Segments resulting in two levels of service; the Precise Positioning Service (PPS) for military use, and the Standard Positioning Service (SPS) for civil use.¹⁹ As previously described, the Control Segment interfaces with each GPS satellite to ensure the accuracy and health of the constellation, while individual GPS satellites calculate and transmit data to the User Segment to facilitate PNT service.²⁰ To enable PNT service each satellite generates and transmits three things: GPS time , a NAV message data, and three Pseudo Random Noise (PRN) ranging codes.²¹

NAV message data and GPS time (time of transmission) provide GPS receivers information about satellite health, satellite position, satellite transmission time, and Ionospheric delay effects.²² The PRN ranging codes enable GPS receivers to measure the transit time of the PRN signals for each satellite.²³ The three PRN ranging codes are the precision (P) code, which

is the principal ranging code; the Y-code, which is an encrypted P code used by the military; and the coarse/acquisition (C/A) code, which is used as a civil ranging signal and for acquisition of the P (or Y) code [denoted as P(Y)].²⁴ The C/A code is primarily intended for civil use while the P(Y) code is for military use.²⁵ Each satellite broadcasts the three PRN ranging codes with a superimposed NAV message over two radio channels using a Helix Array antenna.²⁶ The C/A and the P(Y) ranging codes are both broadcast on the L1 radio channel at 1575.42 MHz; while the P(Y) signal is broadcast on the L2 channel, at 1227.60 MHz.²⁷ Figure 5 illustrates this process.

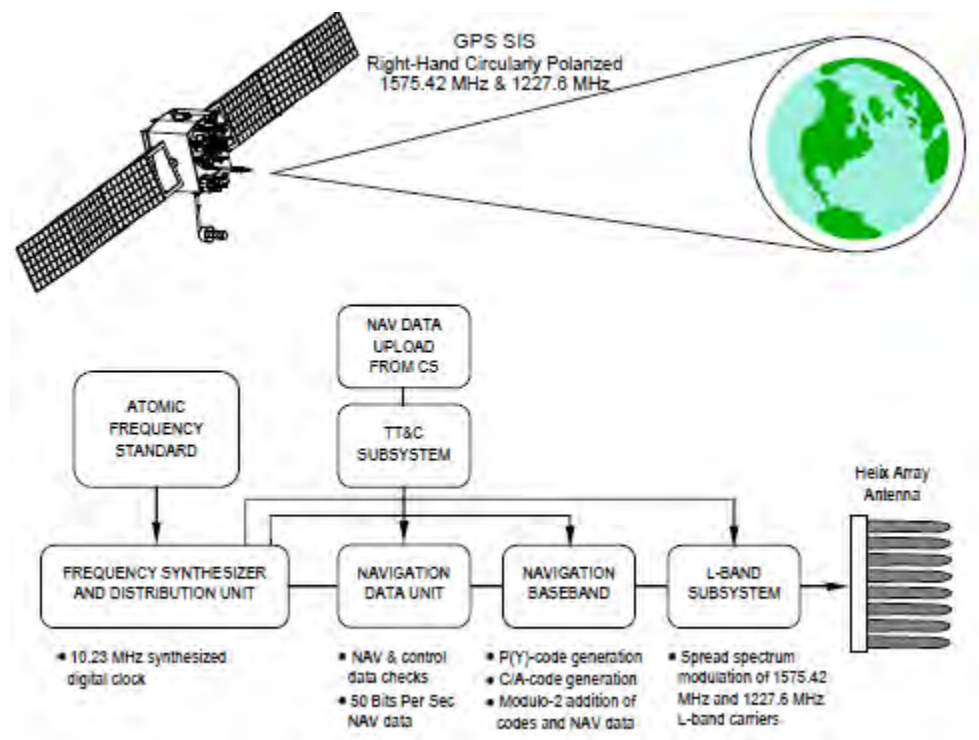


Figure 5. GPS Signal in Space (SIS) Generation and Transmission²⁸

Source: U.S Dept of Defense, Global Positioning System Standard Positioning Service Performance Standard, 4th Edition, (Sept 2008), p 4, <http://www.gps.gov/technical/ps/>

GPS receivers in view of a satellite's signal(s) determine three measurements; the current time, the position of the satellite, and the time delay of the signal.²⁹ These measurements are

derived from the NAV data message and the PRN code(s) broadcast over the L1 and L2 signals.³⁰ The NAV data message is used to calculate the current time and the position of each satellite at the time the signals were transmitted.³¹ As previously described, the ranging codes enable a GPS receiver to measure the transit time of the PRN signals for each satellite. GPS receivers measure the time delay between when the satellite sent the signal and the local time when the signal was received to determine the range between each satellite and the receiver.³² Conceptually, each range measurement defines a sphere centered on a GPS satellite.³³ The common intersection point of the sphere on or near the earth's surface defines the receiver's position.³⁴ However, for accurate GPS positioning, a minimum of four satellites (spheres) are normally required to be simultaneously in view of the receiver.³⁵ By comparing each satellites position and range, the receiver can accurately determine its position.³⁶

Inferences – GPS Structure and Functionality

The overview of GPS structure and functionality provided above reveals several inferences pertinent to this study. First, GPS PNT service is dependent on effective communications between the space segment and the user segment via the radio frequency. Like any radio signal, the L1 and L2 bands used by GPS work when line of sight is established between the GPS receiver and not less than four satellites. However, as with any other radio frequency, GPS signals can be subject to interference; natural or manmade, deliberate or unintentional. Second, the control and space segments can be aptly described as critical segments which contain low density infrastructure. For example, the control and space segments are limited to two master control stations, sixteen satellite antennas, and 31 operational satellites. A disruption or denial of functionality to either the control or the space segments could cause

catastrophic effects to GPS service in the event of a natural disaster or enemy action. It is with these inferences in mind that the study segues to an examination of the Anti-GPS threat.

The Threat Environment

Throughout the contemporary environment, current and potential adversaries have a wide variety of Anti-GPS capabilities available to utilize against a MAGTF and its support structure. Anti-GPS threats range in shape, size, and purpose. Most Anti-GPS threats can be employed in both conventional and irregular warfare and at different stages of hostility. Moreover, a variety of Anti-GPS capabilities are available to both state and non-state adversaries. For the purpose of this study, Anti-GPS threats are grouped into four major categories: GPS jamming, GPS Spoofing, cyber attack, anti-satellite weapons, and kinetic attacks. Jamming and spoofing attacks are generally directed at the User Segment and focus on denying, disrupting, or deceiving a GPS receiver's use of GPS signals. Anti-Satellite weapons and kinetic attacks are generally directed at either the space and/or control segments with the purpose of destroying or neutralizing the functionality of each. Cyber attacks can be directed at any of the GPS segments with the intent of disrupting or disabling the functionality of components or the network. Each Anti-GPS threat has the potential to affect different systems within a MAGTF. Therefore, the following sections of this study describe the nature and capabilities of each threat in further detail beginning with perhaps the most prevalent of the Anti-GPS threats, GPS jamming.

GPS Jamming

What is GPS Jamming?

GPS jamming is arguably one of the most likely and most effective Anti-GPS threats to be utilized against a MAGTF. GPS jamming is a form of electronic attack which is used to disrupt or deny the reception of radio frequencies broadcast by GPS satellites to GPS receivers.

The effects of GPS jamming can influence activities at the tactical and operational levels of war and are certain to impact the civil use of GPS. Jamming works by using various signals that directly affect electronic systems being targeted, namely in the case of GPS the receiver.³⁷

Jamming signals are electromagnetic emissions produced by a jammer with the appropriate amplitude, frequency, phase, polarization, space and time characteristics to effect (GPS) receivers.³⁸ Two of the more common jamming signals are destructive and masking signals.³⁹

Destructive jamming signals use high energy, electromagnetic radiation to cause irreversible damage to input components in the receiver of the target being jammed.⁴⁰ Whereas masking jamming signals act on both the receiver and the signal to exclude / hinder the receivers ability to detect useful signals in order to cause a temporary effect.⁴¹

Proliferation and Effectiveness

To conduct jamming, both nation states and non-state actors have a variety of commercial and military grade GPS jamming devices available. Jammers come in all shapes and sizes ranging from the size of a cell phone to vehicle mounted jammers. Jammers also vary widely in terms of capability, cost, and effectiveness. Many military grade GPS jammers are produced by companies based in countries to include China, Russia, Switzerland, and the Kingdom of Jordan. However, jammers are widely available for export and not exclusively found only in the country of manufacture. Jammers can easily and affordably be procured by states, individuals, and organizations in nations that have no laws governing the sale of GPS jammers. Table A highlights some of the GPS jammers available on the export market.

Table A. Examples of GPS Jammers

Jammer Nomenclature	Capabilities	Company	Country of Origin
Aviaconversiya Jammer	<ul style="list-style-type: none">• Jam GPS navigation• Jam precision munitions	Aviaconversiya	Russia ⁴²
WaveStorm	<ul style="list-style-type: none">• Jam GPS navigation	Jordan Electronic Logistics Support	Jordan ⁴³
SAJ-1030	<ul style="list-style-type: none">• Jam GPS navigation• Jam precision munitions• Defeat GPS receivers anti-jammer countermeasures	Albrecht Telecommunications	Switzerland ⁴⁴
AURA	<ul style="list-style-type: none">• Jam GPS navigation• Jam mobile communications channels	Novo Corporation	Russian ⁴⁵

The recent history of GPS jamming shows a growing utilization of GPS jammers by rogue nations to defeat or deny the use of GPS technology. For example, during the 2003 U.S. led coalition invasion of Iraq, Saddam Hussein reportedly utilized GPS jammers procured from the Russian company Aviaconversiya to protect several of the regimes critical sites.⁴⁶ More recently, North Korea (allegedly) used GPS jammers against South Korea on three occasions; August 2010, March 2011, and April 2012.⁴⁷

Each of these cases raise issues concerning the military application and effectiveness of GPS jammers. During the most recent incident between North and South Korea, GPS service to 670 commercial flights and 110 merchant shipping vessels was disrupted.⁴⁸ However, the South Korean military claims it was not impacted because the South Korean military does not rely on GPS.⁴⁹ On the other hand, during Operation Iraqi Freedom the company supplying the Iraqi's jamming systems (Aviaconversiya) claims their jammer technology was effective in jamming precision munitions in jammer protected areas. However, the U.S. led coalition claims Iraqi GPS jammers had no impact on operations.⁵⁰

The opposing claims regarding the effect GPS jamming has on military uses for GPS are both valid to an extent. It is theoretically possible that GPS jammers can be effective in jamming even military grade GPS receivers. However, it is also possible that even though jammers work as designed, they yield no impact on the operations of an opposing force. This was probably the case in Iraq during 2003 where the net effect of GPS jammers was likely irrelevant against the systematic destruction of other systems upon which GPS jammers are either integrated with or reliant upon. However, it is probable that smaller scale MAGTF operations such as those conducted by a Marine Expeditionary Unit (MEU) may not be able to mitigate the net effect of GPS jamming due to limited resources. Nevertheless, what cannot be ignored is that GPS jammers can cause significant issues for infrastructure supporting critical civil functions. GPS jamming can place many of these civil functions at an increasing risk and in doing so adversely impact or conflict with ongoing military operations. For example, adversary nations and non-state actors can effectively use GPS jammers to disrupt civil use for the purpose of creating a more chaotic environment and causing additional challenges during MAGTF operations in the areas of civilian aircraft travel and navigation on waterways.

Nevertheless, one of the major weaknesses of GPS jammers is the method in which they work. In order to disrupt a GPS signal, most jammers create a powerful signal to drown out the satellite signal. However, in doing so, the jammer is broadcasting a signal which is traceable to the jammer's antenna and therefore can be used as a way to target the jammer through electronic warfare or strike. Ultimately, the effectiveness of GPS jammers is reliant on an effective integration with other jammers and force protection measures such as air defense. In the same way that the U.S. has improved its ability to defeat GPS jammers since OIF through its advances in electronic countermeasures, competitor nations and adversaries alike will endeavor to improve

their capabilities and ensure GPS jamming is improved and better integrated with other defensive or offensive measures to be more effective.

GPS Spoofing

What is GPS Spoofing?

GPS spoofing, like GPS jamming, is form of electronic attack against the user segment. However, unlike GPS jamming where the signal is blocked, with GPS spoofing the targeted receivers are deceived.⁵¹ GPS spoofing works by creating a false GPS signal that tricks a GPS receiver into tracking a counterfeit signal(s).⁵² GPS “spoofers” are the devices that create false GPS signals to fool receivers into thinking that they are at a different location or different time.⁵³

Proliferation and Effectiveness

Although spoofing is feasible for nation states, organizations, and non-state actors it remains a sophisticated form of electronic attack with significant challenges to overcome which requiring appropriate subject matter expertise. Furthermore, spoofing attacks against encrypted military GPS signals presents an extremely difficult challenge. As a result, an effective threat from spoofing against a MAGTF is considered unlikely except against peer competitor nation states.

Cyber Attack

What is a Cyber Attack on GPS?

Another rapidly increasing threat to GPS comes in the form of cyber warfare. Warfare across the cyber domain presents several opportunities for both nation state and non-state actors interested in disrupting or denying the military and/or civil uses of GPS. In fact, great potential exists for cyber attacks using highly sophisticated adaptations of malware and viruses to disrupt or degrade GPS segments. Malware and viruses can alter the software of operating systems or

components onboard GPS satellites, receivers, or the master control station to cause system failures and other designed manipulation of systems. At present, many of the ways and means to engineer and execute an effective cyber attack against military uses of GPS requires the resources that can only come from a nation state. However, due to rapidly advancing technology and innovation, the opportunity will continue to increase in the future for non-state actors and rogue organizations to carry out effective cyber attacks against military and civil uses of GPS technologies.

Cyber Attack Feasibility Experiment

This future is evident in the results of a recent experiment by researchers at Carnegie Mellon University and Coherent Navigation. The 2012 experiment focused on the potential for conducting cyber attacks against the civil uses of GPS. The research showed that GPS could be subject to cyber attack via several means to include; manipulating the NAV message of the GPS signal, accessing the root operating system on a GPS receiver, and synthesizing new PRN code offsets.⁵⁴ The experiment effectively demonstrated that cyber warfare could be a highly effective means to attack an unencrypted GPS signal and components. Furthermore, the experiment showed what could be achievable with very limited resources (\$2,500 in equipment) and the right subject matter expertise.⁵⁵ In exposing the vulnerabilities of the civil uses of GPS technology to cyber attack the study can infer possible implications regarding the military use of (encrypted) GPS technology. Namely, that any well resourced adversary with subject matter expertise can present a formidable threat to the military uses of GPS using cyber warfare to defeat the protections of an encrypted L2 signal or by taking over operational control of GPS satellites.

Anti-Satellite Weapons

Scope and Capabilities

Unlike jamming and cyber attacks, the capability of Anti-Satellite weapons is currently limited to only a few nation states. China and Russia are among the nations who are aggressively developing Anti-Satellite weapons programs that utilize rockets or lasers to destroy or disable GPS satellites.⁵⁶ China's Anti-Satellite weapons program has received continued attention in recent years and is regarded by some experts as being the most advanced.⁵⁷ The Chinese program, known as DN-2, is believed to have the capability of destroying satellites in high geostationary orbits (appx. 20,000 km).⁵⁸ The development of this program enables China to strike U.S. satellites within the GPS constellation.⁵⁹ In fact, recent testing by the Chinese in 2007 and 2011 demonstrated a capability to hit an aging Chinese meteorological satellite and a designated point in space.⁶⁰

Effectiveness and Probability of Use

Anti-Satellite weapons increasingly represent a critical threat to both the civil and military uses of GPS. However many anti-satellite programs, to include the Chinese program, lack of transparency thus making an accurate threat assessment difficult.⁵⁷ Nevertheless, the potential use of Anti-Satellite weapons remains unlikely with the exception of a scenario involving total war between superpowers such as the U.S., China, or Russia. The greater significance of these programs for the United States is the realization that other nations recognize how heavily reliant the U.S. military is on GPS technology to carry out critical functions.⁶¹ Their willingness to invest capital and resources into Anti-Satellite programs reflects what this study regards as an interesting ambition that may provide a glimpse into their long term strategic outlook towards how they view future relations with the United States.

Kinetic Attack

What is a Kinetic Attack on GPS?

For the purposes of this study, kinetic attack encompasses methods undertaken by a nation state, organization, or non-state actor to destroy or neutralize the critical infrastructure comprising the GPS control segment such as the master control station and ground antennas. Kinetic attack may include the use of bombs, missiles, explosives, direct fire weapons or a combination of two or more methods.

Nation State and Non-State Actor Capabilities

Superpower nation states have the capability of using Inter-Continental Ballistic Missiles (ICBMs), air strikes, Special Forces and other irregular techniques. Rogue nations are likely to utilize less advanced methods to conduct kinetic attack to include special operations or sabotage via a non-state organization. Non-state actors or international terrorist organizations acting independent of a nation state are likely to employ irregular methods such as car and truck bombings or a dirty bomb. Although nation states and non-state actors generally have different means available to them for conducting kinetic attack, no one particular means is exclusive to either the state, organization, or individual with the exception of Inter-Continental Ballistic Missiles or air strikes. However, regardless of the nature of kinetic threat, this type of Anti-GPS capability can be effectively employed by a variety of actors and at all points along the spectrum of conflict.

Inferences – The Threat Environment

As evidenced, a variety of threats can interfere with the functionality of GPS and Table B summarizes several of their important characteristics. In addition, there are four major inferences to draw from an analysis of the threat environment. First, the range of Anti-GPS capabilities is multifaceted and can threaten the functionality of one or all GPS segments depending on the adversary and nature of conflict. The application of these threats spans across

the spectrum of conflict and presents unique operating challenges and mission constraints for MAGTFs ranging in size from a MEU to a MEF. Second, Anti-GPS capabilities can originate or operate well outside a MAGTF's area of operations or ability counteract. The capabilities of Anti-Satellite Weapons, Kinetic Attacks, and Cyber Attacks illustrate this point. Third, not all Anti-GPS capabilities directly target the MAGTF; however, all Anti-GPS capabilities share the same goal which is to interfere with the functionality of GPS PNT services. As a result, MAGTF operations should be planned and conducted with the recognition for all potential Anti-GPS threats available to an adversary. Recognition of the threat also entails assessing the likelihood of its use and the risk to operations throughout planning and execution. The fourth and final point is, not all Anti-GPS threats are equally capable. Individuals, organizations, and nation states have varying resources and subject matter expertise to lend to the development of Anti-GPS capabilities. For example, military grade Anti-GPS capabilities such as jammers and spoofers will likely achieve different thresholds of effectiveness than those developed by an organization or individual. On the other hand, the effectiveness of cyber attacks and kinetic attacks by non-state actors and organizations presents the possibility to achieve equally devastating effects to those capabilities rendered by a nation state.

Table B. Summary of Anti-GPS Threats

Threat Capability	GPS Segment Targeted	Purpose	User
Jamming	User Segment	Deny / Disrupt GPS signal	Individuals, Organizations, Nation States
Spoofing	User Segment	Deceive GPS receiver	Individuals, Organizations, Nation States
Cyber Attack	User Segment Control Segment Space Segment	Deny, Disrupt, or Deceive GPS	Individuals, Organizations, Nation States
Anti-Satellite Weapons	Space Segment	Destroy GPS satellites	Nation States
Kinetic Attack	Control Segment	Destroy critical GPS infrastructure	Individuals, Organizations, Nation States

Qualitative Assessment

In order to assess the probable effects and implications of the various Anti-GPS threats during MAGTF operations this study examines two vignettes. Each vignette presents a plausible scenario in which a MAGTF confronts one or more Anti-GPS capabilities from a nation state, an organization, or an individual. Each vignette outlines a scenario, the MAGTF's task(s), the enemy situation, and potential enemy courses of action from which probable effects are derived and risk assessed. The risk assessment herein uses a derivative of the Marine Corps Operational Risk Management (ORM) process (outlined in ORM 1-0) and applies modified risk assessment criteria as outlined in Table C. Furthermore, the MAGTF's employment in each situation reflects the formal tasks established in the Marine Corps Task List (MCTL) of MCO 3500.26A W/ CH 1. The vignettes range in complexity beginning with a small MAGTF (MEU sized) performing a single mission against an adversary utilizing a single GPS threat, to a large MAGTF (MEF or MEB sized) performing multiple missions against an adversary with multiple GPS threats.

Table C. Risk Assessment Description

Severity	Description
Critical	The MAGTF is unable to conduct the mission / execute operations due to the use of Anti-GPS capabilities. A different COA will be required. The hazard(s) will disrupt or deny the ability of the MAGTF to employ mission essential GPS enabled systems or equipment. Activities across one or more Warfighting Functions are impaired. The operational capability of the MAGTF is impaired.
Serious	The MAGTF is required to alter some portions of the concept of operations or adjust TTPs in order to conduct the mission due to the use of Anti-GPS capabilities. Some activities within a Warfighting Function may become impaired; however, the function remains capable but with significantly increased risk to people and systems.
Moderate	The MAGTF remains mission capable across all Warfighting Functions; however, the temporal impairment of certain activities may occur due to the use of certain Anti-GPS capabilities.
Negligible	The MATGF remains mission capable across all Warfighting Functions. The effects of Anti-GPS capabilities do not significantly impair operational capabilities.

Vignette 1: MEU Mission

The first vignette involves a MEU preparing to conduct Marine Corps Task (MCT) 6.2.1 (the) Tactical Recovery of Aircraft Personnel (TRAP.)⁶² TRAP missions require a MEU to respond on short notice and enter hostile territory to recover downed aircrews. TRAP missions, like other types of MEU missions such as amphibious raids or amphibious assault, are regarded as high risk due to the potential for enemy opposition and the limited number friendly combat forces ashore. During the last 20 years, MEUs have conducted two TRAP missions for downed U.S. aircrews over hostile territory.

The most well known TRAP mission was over Bosnia in 1995 to rescue Air Force Captain Scott O’Grady while a second more recent TRAP mission over Libya in 2011 was to rescue the crew of an F-15 fighter jet.^{63, 64} Based on published accounts and equipment used to support the Bosnia and Libya TRAP missions, it is reasonable to assert that both missions succeeded in part because GPS technology assisted in the effort to locate the downed aircrew(s) and navigate the TRAP mission aircraft.^{65, 66, 67} The following scenario uses a hypothetical TRAP mission to analyze how Anti-GPS capabilities may affect MEU missions, such as TRAP, in the future.

Situation

Six months ago, Country “X” launched a military incursion into neighboring Country “Y” over long disputed territorial claims. International pressure and a brief coalition air campaign forced the withdrawal of Country “X” from Country “Y”; however, tensions remain high while long term peace negotiations ensue at the United Nations (U.N.). U.S. and coalition partners have been enforcing a U.N. no fly zone over Country “X” for approximately one month and have shot down two military aircraft from Country “X” violating the no fly zone. These engagements have increased resentment against the U.S. and Country “X” has vowed retaliation. Less than an hour ago, a U.S. F-15 jet was shot down over Country “X” by an unknown variant of surface to air missile. The location of the aircrew is believed to be in a heavily wooded, rural area approximately 90 nautical miles from the coast of the Mediterranean Sea. A second F-15 on the sortie reported seeing both pilots eject and chutes deployed. A short radio transmission from one pilot indicated some injuries, while the disposition of the second pilot is unknown. A MEU is on standby off the coast and is preparing to execute a TRAP mission once approval is granted.

Enemy Forces / Course of Action

Country “X’s” military force is at approximately 65% readiness following combat operations in Country “Y” and the coalition air campaign. The military is comprised of both conventional and paramilitary forces. They are equipped with a mixture of old and new weapons from the Russian Federation and Soviet Era. The shoot down of the F-15 reveals that Country “X” still retains a variant of effective surface to air missiles battery’s (SA-9 or SA-11) which were previously thought destroyed during the coalition air campaign. Furthermore, Country “X” is suspected of having recently acquired and tested over a dozen GPS jammers in a new effort to disrupt coalition air patrols enforcing the no-fly zone and coalition use of precision guided munitions.

The shoot-down of the F-15 jet is part of a new strategy by Country “X” to gain additional leverage during negotiations at the U.N.. Country “X” will attempt to capture the downed air crew to be used as bargaining chips to gain a more favorable settlement. The most likely course of action for Country “X” is to utilize GPS jammers to disrupt and delay U.S. efforts to locate and rapidly recover the downed aircraft personnel in order to buy enough time to find and capture pilots themselves. The most dangerous course of action for Country “X” is to utilize GPS jammers in conjunction with Anti-Aircraft weapons to ambush the TRAP rescue force while enroute to recover the downed F-15 air crew. In doing so Country “X” may be able to capture additional U.S. or coalition personnel to use as political/diplomatic leverage.

Effects Assessment

While the effects of GPS jamming are not always certain, military grade GPS jammers such as those used by countries like North Korea have demonstrated the ability to interfere with military activities or technology using GPS.⁶⁸ Therefore, it is reasonable to assert that an unmitigated GPS jamming threat presented in this scenario would be effective against multiple

systems and equipment used by the MEU and the downed aircrew during a TRAP mission. Table D shows the munitions, systems, and equipment within the TRAP mission that would likely be affected by GPS jamming. The various platforms are grouped according to their Warfighting function in order to show the impact between similar systems and the capability they collectively provide to the MEU / TRAP mission.

As Table D shows, GPS jamming can affect TRAP force aircraft, fighter escorts, refueling aircraft, precision munitions, and aircrew survival radios. However, the effectiveness of jamming and the degree of severity on each Warfighting function is varied. The severity of the effect is determined by factors to include; the role of GPS within the activity affected, the nature of the task in relation to the mission (critical or non-critical task), and the availability of alternate techniques to perform the same task as GPS. Arguably, the most critical factor in determining the severity of jamming is whether or not an alternate technique can be used in place of GPS to perform the same GPS task. While having alternative to GPS technology does provide flexibility and options it does not provide mission assurance. For example, alternatives to GPS may not be trained to standard or they may be undesirable to use under the circumstances of the mission. In addition, the implications of jamming more than one system within the same Warfighting function, or across multiple Warfighting functions, can create a compounding effect within that activity and reduce the capacity of the MEU to perform a certain task. In doing so, the cumulative effects can create severe implications for the MEU's TRAP force. Three significant implications result from the effects of GPS jamming in this scenario.

Table D. Potential Effects of GPS Jamming on TRAP Mission Capabilities

	GPS Navigation Systems effected by GPS Jamming	Targeting Systems effected by GPS Jamming	Munitions effected by GPS Jamming	Potential Effect on WarFighting Function	Severity of Effect on Warfighting Function
Maneuver	- CH-53, MV-22 (TRAP force)	-	-	Maneuver is Degraded. Analog navigation available.	Serious
Intelligence	- Unmanned Aerial Vehicles (UAV's): Shadow, Scan Eagle	- UAV's: Shadow, Scan Eagle	-	Intelligence is Degraded. Alternate ISR means available.	Moderate
Fires	- AV-8B, AH-1, UH-1	- LITENING Targeting Pod	- Joint Direct Attack Munition (JDAM)	Fires are Degraded. Retain use of analog instruments & general purpose bombs.	Serious
C2	- PRC-112 (internal GPS receiver)	-	-	C2 is Degraded. PRC-112 retains voice communications.	Moderate
Logistics	- KC-130 Refueler (if available)	-	-	Logistics is Degraded. Analog navigation available. Refueling mission not impacted.	Negligible
Protection	-	-	-	Mission Capable	-

First, GPS jamming would impede most efforts to quickly locate the downed aircrew.

GPS technology in the PRC-112 survival radio of the aircrew and other search and rescue aircraft such as UAV's flying reconnaissance would be impaired by jamming. This would result in uncertainty about the location of the aircrew that would likely affect the decision of when or whether or not to conduct the TRAP mission. Any excessive delay to launching the TRAP mission only increases the likelihood that the aircrew will end up in the hands of the adversary.

Second, GPS jamming would negate the advantage of GPS precision fires such as JDAM's. Precision fires enhance support to the TRAP force by creating a greater standoff

distance between friendly aircraft and enemy anti-aircraft weapons. Precision fires also allows for first round effects on target and minimizes collateral damage. By degrading the TRAP force's ability to use precision fires, the enemy effectively closes the gap between fighter escorts and anti-aircraft weapons thereby leveling the playing field for the enemy.

Third, GPS jamming would negate the effective use of GPS navigation systems for aircraft in support of the TRAP mission. This would create a decision point of whether to fly the mission at night or during the day. With either option (day or night), pilots retain the ability to navigate using analog instruments. However, their ability to fly low and fast over hostile territory at night while avoiding anti-aircraft threats would significantly increase the risk to their mission. Although, flying during the day would increase the ability of the pilot to navigate and maneuver the aircraft, the aircraft would be more susceptible to anti-aircraft threats. In either case, the MEU commander would have to carefully weigh the risks of flying during the day against those of flying at night.

The effects of GPS jamming in this scenario degrade the capability of the MEU across five Warfighting functions. Although the MEU retains the capacity to conduct the TRAP mission, an increased risk to both the TRAP force and supporting activities results as previously discussed. As Table E shows, this threat is assessed to pose an overall serious risk to the mission. What is already a dangerous mission became even more risky due to the threat from GPS jamming. The effects of jamming ultimately lengthen the time to locate and recover the downed air crew and force the use of more risky, less desirable options by the TRAP mission force. These implications increase the probability of mishap, death, or mission failure.

Table E. GPS Jamming Risk Assessment

Overall Risk to Mission (Unmitigated)	
Critical	
Serious	X
Moderate	
Negligible	

Vignette 2: MEF Operations

The second vignette presents a scenario involving high intensity conflict operations, a large scale MAGTF (MEF sized), and an adversary nation with a multifaceted Anti-GPS capability. The large scale operations outlined in this vignette encompass virtually every Marine Corps Task from the MCTL and multiple subtasks too numerous to list herein.⁶⁹ The purpose of this vignette is to demonstrate the effects and implications of Anti-GPS capabilities in support of large scale, high intensity conventional operations. Although small and mid-intensity conflicts may be more likely in the future, there are innumerable variables associated with them which prevent the complete array of Anti-GPS threats to be sufficiently examined. Furthermore, large scale operations involving conventional warfare are by no means a thing of the past. American participation in wars and conflicts such as World War II and the 1991 OPERATION Desert Storm demonstrate that U.S. military involvement can quickly ramp up and the future use of large MAGTF's such as MEB's and MEF's remains a imperative requirement. However, as with MEU sized operations, MEF operations may also become increasing difficult as the range of Anti-GPS threats increases.

Situation

Three years ago Country "A" elected a new head of state following eight years of economic depression and widespread public discontent with the government. The president and

his National Socialist party promised to usher in a new era of prosperity and a return to the nation's preeminence as a world superpower. The new president and his ruling party formed a majority in parliament and quickly enacted sweeping changes by increasing state control of the economy, rapidly expanding the size of the military, and developing or acquiring new military arms capabilities. They also re-instituted many of the country's old diplomatic policies and rhetoric which held very strong Anti-Western and U.S. views, reminiscent of the cold war era.

Furthermore, the president, an ethnic Slav, revived long held territorial claims to an oil rich region in one of Country "A's" southern neighbors, the nation state of Country "B".

Country "B" has a minority population of Slav's which formerly held the ruling majority in Country "B" from the end of World War II until the early 1990's. Country "B", now fiercely independent and a member of NATO, has a healthy economy, a small but capable military, and is the largest exporter of petroleum in the region.

Three weeks ago, without provocation, Country "A" invaded Country "B" using air and land forces. Although, Country "B's" armed forces were initially overwhelmed, their lines have stabilized and a pocket of effective resistance extends about 40 miles north of their capital city on the Black Sea. The situation remains desperate for Country "B" and they have called on the international community for military assistance.

Although international condemnation has been almost unanimous; Country "A" has refused to withdraw its forces and is threatening retaliation against any nation interfering with their operations. The call for immediate action was unanimous among NATO member nations and received a majority of support in the United Nations. The United States, Great Britain, and France offered the most responsive military options and forces are underway to form a Combined Amphibious Task Force centered around a Marine Expeditionary Force. The intent

for the MEF and allied militaries is to rapidly transition combat power ashore into areas controlled by Country “B”, reinforce the armed forces of Country “B”, and set conditions for follow-on NATO forces.

Enemy Forces / Course of Action

Country “A” has a large land army with 1,000,000 personnel, a navy with 200,000 personnel and an air force with 300,000 personnel. The modernization and rebuilding of their armed forces has provided Country “A” with some of the most capable battlefield weapon systems and technologies. Several programs and systems were specifically designed to counter U.S. capabilities. Among the most notable programs and systems are their cyber warfare program, new radars which purportedly can detect U.S. stealth aircraft, a series of long range precision ballistic missiles (believed to be anti-satellite missiles), and an array of electronic warfare capabilities to include frequency hopping jammers and GPS jammers. Country “A” also has an inventory of nuclear, chemical, and biological weapons programs; however, their use is considered not probable due to economic, environmental, and political implications.

Although the armed forces of Country A are highly regarded, their leadership is suspected of wanting to avoid a direct military confrontation with U.S. and NATO forces and is surprised at the resolve from the international community. The country’s political leadership is concerned that an extended period of war will lead to domestic political repercussions and an economic downturn which would erode the power of the ruling political party. However, to buckle under the threat of NATO military pressure would also be perceived as weakness within the ruling party’s support base. In an effort to deal with both concerns, Country “A” is expected to defend its territorial gains within Country “B” for as long as possible by deterring the use of military force by NATO. To achieve deterrence, they will utilize a combination of capabilities

beginning with cyber and electronic warfare methods and escalating if necessary to unconventional warfare and the use of anti-satellite weapons.

The most likely course of action for Country “A” is to utilize a combination of GPS jamming and cyber attacks on GPS segments to disrupt and deny the use of GPS by NATO forces prior to their engagement in combat against Country “A”. The most dangerous course of action for Country “A” will be to conduct kinetic attacks using Anti-Satellite weapons and sabotage to destroy the critical infrastructure within the control and space segments of GPS. In pursuing either course of action, Country “A’s” objective is to remove the marked advantage provided by GPS to NATO and compel NATO and the international community to reconsider pitting a degraded military alliance against their armed forces who would then hold equal footing.

Effects Assessment

As described, Country “A” is capable of utilizing several Anti-GPS capabilities against the combined force. These capabilities provide direct and indirect methods to affect GPS supported activities across the MEF’s Warfighting functions. The direct threats to the MEF come from adversary capabilities such as GPS jamming. The indirect threats come from the use of cyber attacks, anti-satellite weapons, and kinetic attacks on the space and control segments of GPS itself. Table’s F and G show the potential range of effects that an unmitigated set of Anti-GPS threats could bear upon the MEF. Table F shows the potential effects of GPS jamming on the MEF, while Table G shows the effects of cyber attack, kinetic attack, and anti-satellite weapons on the space and control segments of GPS.

As previously explained during the TRAP mission vignette and reflected in Table F, GPS jamming has the potential to degrade navigation systems, targeting systems, and precision

munitions. The degraded functionality of these activities would result in severely adverse effects on the MEF during high intensity conflict operations. Of particular concern is the severity of effects on the functions of maneuver and fires. The effects on maneuver would be critical due to a degraded capacity to maintain situational awareness of friendly and enemy unit locations. The resulting lag would erode operational tempo and slow the MEF's ability to conduct fires. In addition, the effectiveness of precision munitions would in all probability be severely degraded. This would result in additional sorties or additional artillery fire missions to service targets. These effects would increase ammunition expenditures, aircraft fuel expenditures and the exposure of friendly artillery to enemy counter-fire.

Table F. Potential Effects of GPS Jamming on the MEF

	GPS Navigation Systems effected by GPS Jamming	Targeting Systems effected by GPS Jamming	Munitions effected by GPS Jamming	Potential Effect on Warfighting Function	Severity of Effects on Warfighting Function
Maneuver	- Aircraft: CH-53, CH-46, MV-22 - DAGR equipped combat vehicles (or personnel): M1/A2, LAV, AAV, MRAP, HMMWV	-	-	Maneuver is Degraded. Retain use of analog instruments and manual navigation techniques.	Critical
Intelligence	- UAVs: Shadow, Scan Eagle - Tactical Hydrographic Survey Equipment (THSE)	- UAVs: Shadow, Scan Eagle	-	Intelligence is Degraded. Inertial Navigation onboard must be used.	Moderate
Fires	- Aircraft: AV-8B, AH-1, F-18, UH-1 - Cannon Artillery: M-777 (DAGR equipped) - Rocket Artillery: M-142 (DAGR equipped)	- LITENING Targeting Pod - Target Location, Designation, And Hand-Off System (TLDHS)	- JDAM - GMLRS - Excalibur - PERM (future)	Fires are Degraded. Retain use of analog instruments & general purpose bombs / munitions.	Critical
C2	- Blue Force Tracker - DAGR - Radios: AN/PRC 117, Handheld Radio Family of Systems (HRFS)	-	-	C2 is Degraded.	Serious
Logistics	- KC-130 - DAGR equipped resupply Vehicles: MTVR	-	-	Mission Capable.	Negligible
Protection	-	-	-	Mission Capable.	-

Although the effects of GPS jamming can be severe, the indirect threats shown in Table G pose more dire implications to the MEF. Unlike jamming or spoofing which target the user

segments, anti-satellite weapons, kinetic attack and cyber attacks target the control and space segments. As described previously, the effects from these Anti-GPS threats have the potential to render GPS disabled indefinitely. In doing so, the effect of denying GPS use to the MEF is achieved, but with sustained effects and long term implications. The destruction of the MCS, AMCS, GA's, or GPS satellites would be clear cuts acts of war. However, if the attacks achieved the element of surprise, they would stun the United States and allies while degrading their collective ability to retaliate. In doing so, the probability of Country "A" deterring the use of military force against it would be significantly increased.

Table G. Potential Effects of Anti-GPS Threats on the GPS Control & Space Segment

	Potential Effects of Cyber Attack	Potential Effects of Anti-Satellite Weapons	Potential Effects of Kinetic Attack	Severity of Effects on GPS Segment
Space Segment	Disrupt / Disable onboard satellite components. Impair functionality of PNT service	Destroy / Disable satellites	-	Critical
Control Segment	Disrupt command and control systems	-	Destroy / Disable ground antennas and MCS / AMCS	Critical

The effects from the multitude of threats in this scenario degrade the capabilities within five of six Warfighting functions and destroyed, disabled, or disrupted the control and space segments of GPS. Moreover, these threats achieved either serious or critical effects in five of the eight functions assessed as shown in Table's F and G. Therefore, as Table H reflects, the cumulative effect of these threats pose an overall critical risk to the MEF's mission and ability to bring the fight. Although high intensity conflict operations are inherently dangerous and laden

with risk, the effects resulting from the use of Anti-GPS threats would certainly jeopardize the MEF mission.

Table H. MEF Risk Assessment

Overall Risk to Mission by multiple Anti-GPS Threats (Unmitigated)	
Critical	X
Serious	
Moderate	
Negligible	

Inferences – Qualitative Assessment

The effects from the two vignettes provide solid evidence that Anti-GPS capabilities can disrupt or deny the use of GPS within a MAGTF. Anti-GPS capabilities can achieve disruptive effects by directly targeting the MAGTF's systems, capabilities, and munitions or by targeting the GPS control and space segments as an indirect means. However, regardless of the means utilized by an adversary, this qualitative assessment suggests the probable effect of Anti-GPS threats will result in a serious to critical risk levels that will jeopardize the mission and combat effectiveness of the MAGTF under many situations. This increased risk is due in part to the groupings or clusters of GPS aided Systems, munitions and equipment within a particular Warfighting function that share the same vulnerabilities from Anti-GPS threats.

Table I summarizes the clusters of GPS-aided systems, munitions, and equipment which are vulnerable to the effects of Anti-GPS capabilities. Given the level of understanding gained through the course of this research study, it is possible to infer the risk posed to these clusters in support of additional MAGTF missions than those covered in the vignettes. Tables J through N assess the probable risk to the clusters of systems munitions and equipment according to the Warfighting function and probable threat during a given mission.

**Table I. Clusters of GPS-aided systems, munitions, & equipment
vulnerable to (unmitigated) effects of Anti-GPS capabilities**

Maneuver Clusters	Fires Clusters	C2 Clusters	Intelligence Clusters	Force Protection Clusters	Logistics Clusters
<p>-Aircraft GPS Navigation Systems: CH-53, CH-46, MV-22</p> <p>-DAGR equipped combat vehicles (or personnel): M1/A2, LAV, AAV, MRAP, HMMWV</p>	<p>- Aircraft GPS Navigation Systems: AV-8B, AH-1, F-18, UH-1</p> <p>- Cannon Artillery Fire Control System: M-777 (DAGR equipped)</p> <p>- Rocket Artillery Fire Control System: M-142 (DAGR equipped)</p> <p>-GPS Aided Munitions: JDAM, GMLRS, Excalibur, PERM (future)</p> <p>-GPS aided Targeting Systems: LITENING Targeting Pod; TLDHS</p>	<p>- Blue Force Tracker</p> <p>- DAGR</p> <p>- Radios: AN/PRC 117, Handheld Radio Family of Systems (HRFS)</p>	<p>- UAV GPS Navigation Systems: Shadow, Scan Eagle, etc</p> <p>- GPS aided, Tactical Hydrographic Survey Equipment (THSE)</p>	n/a	<p>-Aircraft GPS Navigation Systems: KC-130, CH-53, CH-46, MV-22 iso logistics Ops.</p> <p>- DAGR equipped resupply Vehicles: MTVR, HMMWV, etc</p>

Table J. Cluster Risk Assessment for Amphibious/Limited Raid

Anti-GPS Threat	Probable Risk to Maneuver Clusters	Probable Risk to Fires Clusters	Probable Risk to C2 Clusters	Probable Risk to Intelligence Clusters	Probable Risk to Force Protection Clusters	Probable Risk to Logistics Clusters
Commercially available GPS jamming, spoofing, limited cyber warfare	Negligible to Moderate	Negligible	Negligible to Moderate	Negligible	Negligible	Negligible
Military Grade Electronic Warfare (Jamming, Spoofing)	Moderate	Moderate	Moderate	Moderate	Negligible	Negligible
Military Grade Electronic Warfare and Cyber Warfare	Serious	Moderate	Serious	Moderate	Negligible	Negligible
Kinetic attack or Anti-Satellite Weapons	n/a (Threat use not probable during Raid)	n/a	n/a	n/a	n/a	n/a

Table K. Cluster Risk Assessment for Non-Combatant Evacuation Operations (NEO)

Anti-GPS Threat	Probable Risk to Maneuver Clusters	Probable Risk to Fires Clusters	Probable Risk to C2 Clusters	Probable Risk to Intelligence Clusters	Probable Risk to Force Protection Clusters	Probable Risk to Logistics Clusters
Commercially available GPS jamming, spoofing, limited cyber warfare	Negligible to Moderate	Negligible	Negligible to Moderate	Negligible	Negligible	Negligible
Military Grade Electronic Warfare (Jamming, Spoofing)	n/a (Threat use not probable during NEO)	n/a	n/a	n/a	n/a	n/a
Military Grade Electronic Warfare and Cyber Warfare	n/a (Threat use not probable during NEO)	n/a	n/a	n/a	n/a	n/a
Kinetic attack or Anti-Satellite Weapons	n/a (Threat use not probable during NEO)	n/a	n/a	n/a	n/a	n/a

**Table L. Cluster Risk Assessment for Visit, Board,
Search, and Seizure Level II and III (VBSS)**

Anti-GPS Threat	Probable Risk to Maneuver Clusters	Probable Risk to Fires Clusters	Probable Risk to C2 Clusters	Probable Risk to Intelligence Clusters	Probable Risk to Force Protection Clusters	Probable Risk to Logistics Clusters
Commercially available GPS jamming, spoofing, limited cyber warfare	Negligible	Negligible	Negligible	Negligible	n/a	n/a
Military Grade Electronic Warfare (Jamming, Spoofing)	Negligible to Moderate	Negligible to Moderate	Negligible to Moderate	Negligible to Moderate	n/a	n/a
Military Grade Electronic Warfare plus Cyber Warfare	n/a (Threat use not probable during VBSS)	n/a	n/a	n/a	n/a	n/a
Kinetic attack or Anti-Satellite Weapons	n/a (Threat use not probable during VBSS)	n/a	n/a	n/a	n/a	n/a

Table M. Cluster Risk Assessment for Security, Stability, Transition and Reconstruction (SSTR) Operations

Anti-GPS Threat	Probable Risk to Maneuver Clusters	Probable Risk to Fires Clusters	Probable Risk to C2 Clusters	Probable Risk to Intelligence Clusters	Probable Risk to Force Protection Clusters	Probable Risk to Logistics Clusters
Commercially available GPS jamming, spoofing, limited cyber warfare	Negligible to Moderate	Negligible	Negligible to Moderate	Negligible	Negligible	Negligible
Military Grade Electronic Warfare (Jamming, Spoofing)	n/a (Threat use not probable during SSTR Ops)	n/a	n/a	n/a	n/a	n/a
Military Grade Electronic Warfare and Cyber Warfare	n/a (Threat use not probable during SSTR ops)	n/a	n/a	n/a	n/a	n/a
Kinetic attack	Serious to Critical	Serious to Critical	Serious to Critical	Serious to Critical	Serious to Critical	Serious to Critical

Table N. Cluster Risk Assessment for Amphibious Assault

Anti-GPS Threat	Probable Risk to Maneuver Clusters	Probable Risk to Fires Clusters	Probable Risk to C2 Clusters	Probable Risk to Intelligence Clusters	Probable Risk to Force Protection Clusters	Probable Risk to Logistics Clusters
Commercially available GPS jamming, spoofing, limited cyber warfare	Negligible to Moderate	Negligible	Negligible to Moderate	Negligible	Negligible	Negligible
Military Grade Electronic Warfare (Jamming, Spoofing)	Moderate	Moderate	Moderate	Moderate	Negligible	Moderate
Military Grade Electronic Warfare and Cyber Warfare	Serious	Serious	Serious	Moderate	Negligible	Moderate
Kinetic attack and/or Anti-Satellite Weapons	Serious to Critical	Serious to Critical	Serious to Critical	Serious to Critical	Serious to Critical	Serious to Critical

Counterarguments

There are three potential counterarguments to challenge the inferences of this study.

Generally speaking, these counterarguments either call into question the effectiveness Anti-GPS threats and/or bolster the future structure and functionality of GPS. The counterarguments are:

- (1) the offensive capability of some Anti-GPS threats are overstated, (2) existing U.S. countermeasures and defenses can defeat some Anti-GPS threats, and (3) ongoing and future improvements to GPS will negate the effectiveness of many existing and foreseeable threats.

The first potential counterargument rests on the premise that the ability of certain Anti-GPS threats is overstated. Specifically, that claims regarding the effectiveness of cyber attacks, kinetic attacks, and anti-satellite weapons lack substantive evidence and are based more on conjecture than reality. This counterargument can be vigorously argued using three key assertions. First, the U.S. maintains a technological advantage over Anti-GPS programs and hence has superior capabilities. Second, although Anti-GPS capabilities continue to evolve, the U.S. remains ahead of advancements in threat capabilities. Last, claims regarding the effectiveness of Anti-GPS threats should be considered with a dose of skepticism to avoid both the hype and the pitfalls of overestimating the threat.

Although the points comprising this counter argument have their merit and logic, the major weakness with this position is that it has the potential to deduce what is believed about a threat to only that which is measureable or outwardly apparent. In doing so, this counterargument may fail to recognize the element of deception in play by an adversary. The reality remains that short of war, it is difficult to truly ascertain or predict the range of effects for certain Anti-GPS capabilities under wartime conditions. However, the internal validity of claims in this study regarding the capability of anti satellite weapons, cyber, and kinetic attacks recognize the realities of war and are grounded in evidence involving logical assertions and probable conclusions.

A second potential counterargument to the claims of this study is the contention that existing U.S. countermeasures and defenses offer sufficient protection to defeat or negate the effectiveness of Anti-GPS threats. These measures exist for use against threats to include spoofing or jamming. The defensive measure to defeat spoofing consists of an encrypted GPS

signal used when spoofing is probable or detected. The countermeasures against jamming include the use of air strikes or other kinetic means to destroy GPS jammers.

Although the aforementioned measures may be effective to some extent, they may also be defeated or rendered ineffective. For instance, spoofing is difficult to conduct; however, conceptually it is not impossible to achieve.⁷⁰ The concept is analogous to a locksmith fashioning a key to fit a lock. Once the lock is open an actor can potentially influence or replace the data used in GPS. A nation state with adequate research and technological development may develop spoofing technology that can defeat GPS encrypted signals.

With regard to the countermeasure to defeat jamming, conducting airstrikes or kinetic strikes against GPS jammers is difficult and it increases risk to strike aircraft. The first major obstacle to overcome using this countermeasure is to precisely locate the GPS jammer(s). While some jammers are static and easier to target, other jammers like those used by North Korea, are vehicle mounted.⁷¹ Vehicle mounted jammers can both jam and move thereby making the targeting and striking of them more difficult. GPS navigation systems on UAV's would be degraded and the platform rendered ineffective. Strike aircraft may be forced to navigate using analog instruments and GPS guided bombs rendered ineffective.

As evidenced the counterargument that defenses and countermeasures offer sufficient protection to defeat or negate the effectiveness of Anti-GPS threats is fallible. Both defenses and countermeasures have vulnerabilities that offer opportunities for exploitation by adversaries with the appropriate ways and means.

The final counterargument is that ongoing and future improvements to GPS will negate the effectiveness of several existing and foreseeable threats. The premise of this counterargument centers on U.S. plans to modernize (primarily) the military uses of GPS over

the next 17 years. This modernization plan consists of fielding new GPS satellites, new GPS receivers for military use, a more powerful GPS signal for military use (M-Code signal), and improvements to ground control systems.⁷² Beginning in 2012, the plan will cost \$22 Billion (in U.S. dollars, at today's figures) and be implemented in stages until completion in 2030.⁷³

Although the GPS modernization plan offers several needed improvements and protections to GPS, the plan arguably will fall far short of providing assurance against the rapidly evolving array of threats and does little to counter the claims of this study. The first issue undermining the use of this counterargument is the lengthy timeline for the GPS modernization plan. During the next 17 years, the nature of the threat will presumably change and evolve to such an extent that it will jeopardize any benefits gained during the lengthy timeline set forth in the existing plan. Satellites, receivers, and control systems will arguably be facing a whole new set of more capable threats. Therefore, in order to stay ahead of the threat evolution and adaptation, the implementation timeline for GPS upgrades should be accelerated.

A second major issue undermining this counterargument centers on cost. The projected cost today is \$22 billion; however history is replete with examples of long term projects where the cost ballooned over time to far exceed original estimates. Furthermore, the current financial straits looming over the U.S. and Department of Defense do not provide assurances this modernization program will be safe from budget cuts.

Therefore, the counterargument that ongoing and future improvements to GPS will negate the effectiveness of several existing and foreseeable threats is problematic due to the timeline for implementation and possible increases to cost. Contemporary threats are evolving at a more far more rapid pace than during the Cold War and yet the implementation of a 17-year modernization program by its very nature seems to ignore this. It is highly improbable that the

long term modernization program for GPS will outpace the modernization of the threat. As a result the GPS program will accept a high degree of risk in return for marginal benefits from modernizing.

Recommendations

This study offers three recommendations based on its observations and assessment. The recommendations focus on actions internal to the Marine Corps that should increase the combat effectiveness and mission assurance of a MAGTF in a GPS disrupted /denied environment. These recommendations will enable the sustainment of mission critical activities across the Warfighting functions in the event GPS functionality is either critically or seriously affected.

First and foremost, the Marine Corps should ensure that training tasks which utilize GPS, and support critical activities, be written to require that the task be accomplished with and without the use of GPS. Applicable Training and Readiness (T&R) manuals should be reviewed and updated by each military occupational field sponsor, and organizational leaders should ensure proficiency in both individual and unit level training. Emphasis should also be placed on those tasks which support the conduct of Maneuver, C2, Fires, and Intelligence. Proficiency with these training standards is critical because they sustain techniques and skills that if left untrained, are subject to atrophy or perishable altogether. An inability to perform a critical task without the benefit of GPS is necessary in a GPS disrupted / denied environment. Moreover, the requirement and use of non-GPS training standards is arguably the most efficient and cost effect way to provide mission assurance when fighting an adversary employing Anti-GPS capabilities.

A second recommendation is the Marine Corps should ensure diversity in its systems and avoid developing / procuring systems and capabilities that are entirely reliant on GPS. Although this may seem obvious, the High Mobility Artillery Rocket System (HIMARS) and its Family of

Munitions (FOM) serves to demonstrate this issue. HIMARS is a GPS aided artillery weapon system that uses only GPS aided munitions during wartime. These wartime munitions include the M-30 GPS guided rocket (with DPICM), the M-31 GPS guided rocket (HE unitary), and the GPS guided Army Tactical Missile System (ATACMS). As a result, HIMARS and its family of munitions risk being non-mission capable in a GPS disrupted / denied environment. To avert this sort of problem, Marine Corps Systems Command and Combat Development and Integration Division must ensure that the procurement process for systems and munitions includes an assessment of the threat environment and a consideration for likely scenarios and capabilities that can jeopardize the employment and functionality of future GPS aided capabilities. In doing so, the assessment must determine the extent to which critical systems are vulnerable / affected by the range of threats specifically designed to counter GPS functionality. If systems are assessed as being entirely reliant on GPS, then alternate / additional capabilities should be developed as required to ensure mission assurance of the system / munitions.

A final recommendation to carry forward from the results of this study is for the Marine Corps Warfighting Lab (MCWL) to conduct testing and experimentation to gather additional qualitative and quantitative data regarding the effects of Anti -GPS threats and other A2AD threats on a MAGTF's operational capabilities. The results of a MCWL experiment would serve to benefit future training, acquisitions, and operational planning. Furthermore, the lessons learned from a MCWL experiment may be integrated into training offered through the Tactical Training Exercise Group (TTECG), Marine Corps Tactics and Operations Group, (MCTOG), Expeditionary Warfare Training Group (EWTG), and Marine Aviation Weapons and Tactics Squadron One (MAWTS-1).

Conclusion

This study analyzed the dangers posed to a MAGTF by Anti-GPS threats in the contemporary and future operating environment. As shown in this study, a MAGTF's mission will be probably be jeopardized by an adversary using a credible Anti-GPS capability(s.) The increased risk to a mission results from the vulnerabilities in the structure of GPS and the reliance on GPS in the systems, equipment, and munitions used throughout the Marine Corps today.

Nevertheless, the results of this research study are not absolute. Further experimentation and training is recommended in order to properly assess the effects and implications of Anti-GPS capabilities within the small unit level. Additionally, a greater understanding of the threats and of U.S. vulnerabilities is necessary on the part of leaders and planners. Implementing the common sense recommendations in this study, will serve to reduce the operational risk and enhance mission assurance in a GPS disrupted environment. GPS is a critical capability that must be protected; however, the Marine Corps as an institution must remain vigilant to avoid over-reliance on GPS to assure mission success.

End Notes

¹ Congressional Budget Office Study, *The Global Position System for Military Users, Current Modernization Plans and Alternatives*, October 2011, Summary, p 1
www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf

² Department of Defense, *Annual Report To Congress, Military and Security Developments Involving the People's Republic of China 2011*, (Washington, D.C., Office of the Secretary of Defense, May 2011), p2, www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf

³ Department of Defense, *Annual Report To Congress, Military and Security Developments Involving the People's Republic of China 2011*, (Washington, D.C., Office of the Secretary of Defense, May 2011), p2-6, www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf

⁴ “GPS.GOV”, National Coordination Officer for Space Based Position, Navigation and Timing (NOAA) last modified April 12, 2012, <http://www.gps.gov/systems/gps/>

⁵ “GPS.GOV”, NOAA, last modified April 12, 2012, <http://www.gps.gov/systems/gps/>

⁶ “GPS.GOV”, NOAA, last modified April 12, 2012, <http://www.gps.gov/systems/gps/>

⁷ “GPS.GOV”, NOAA, last modified December 7, 2012,
<http://www.gps.gov/systems/gps/space/>

⁸ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 4,
<http://www.gps.gov/technical/ps/>

⁹ “GPS.GOV”, NOAA, last modified December 7, 2012,
<http://www.gps.gov/systems/gps/space/>

¹⁰ “GPS.GOV”, NOAA, last modified December 7, 2012,
<http://www.gps.gov/systems/gps/space/>

¹¹ “GPS.GOV”, NOAA, last modified December 7, 2012,
<http://www.gps.gov/systems/gps/space/>

¹² “GPS.GOV”, NOAA, last modified August 3, 2012,
<http://www.gps.gov/systems/gps/control/>

¹³ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 5,
<http://www.gps.gov/technical/ps/>

¹⁴ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 5,
<http://www.gps.gov/technical/ps/>

¹⁵ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 5, 6
<http://www.gps.gov/technical/ps/>

¹⁶ “GPS.GOV”, NOAA, last modified August 3, 2012,
<http://www.gps.gov/systems/gps/control/>

¹⁷ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 1
<http://www.gps.gov/technical/ps/>

¹⁸ John Merrill, “Patriot Watch VIGILANCE SAFEGUARDING AMERICA”
(Powerpoint Presentation, Department of Homeland Security, Position, Navigation & Timing (PNT) Program Management Office, March 2012), Slide 7
www.gps.gov/multimedia/presentations/2012/03/WSTS/merrill.pdf

¹⁹ U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-5,
<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

²⁰ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 3, A-6 – A8, <http://www.gps.gov/technical/ps/>

²¹ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 3, 4, <http://www.gps.gov/technical/ps/>

²² U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 8, <http://www.gps.gov/technical/ps/>

²³ “Global Positioning System”, GSM Server, <http://www.gsmserver.com/articles/gps.php>

²⁴ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 4, <http://www.gps.gov/technical/ps/>

²⁵ “CSAC Applications”, National Institute of Standards and Technology, Atomic Devices and Instrumentation Group. http://tf.nist.gov/timefreq/ofm/smallclock/CSAC_Applications.html

²⁶ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 3, 4, <http://www.gps.gov/technical/ps/>

²⁷ “Global Positioning System,” GSM Server, <http://www.gsmserver.com/articles/gps.php>

²⁸ U.S Dept of Defense, *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*, (Washington DC: US Dept of Defense, Sept 2008), p 4, <http://www.gps.gov/technical/ps/>

²⁹ “Global Positioning System,” GSM Server, <http://www.gsmserver.com/articles/gps.php>

³⁰ U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-1,1-2, <http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

³¹ U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-2,
<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

³² U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-2,
<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

³³ U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-2,
<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

³⁴ U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-2,
<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

³⁵ U.S. Government, *NAVSTAR GPS User Equipment Introduction*, Sept 1996, p 1-2,
<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

³⁶ “Global Positioning System”, GSM Server, <http://www.gsmserver.com/articles/gps.php>

³⁷ Sergei Vakin, Lev Shustov, Robert Dunwell, *Fundamentals of Electronic Warfare*,
(Norwood, MA: Artech House Inc, 2001), p 61

³⁸ Sergei Vakin, Lev Shustov, Robert Dunwell, *Fundamentals of Electronic Warfare*,
(Norwood, MA: Artech House Inc, 2001), p 61

³⁹ Sergei Vakin, Lev Shustov, Robert Dunwell, *Fundamentals of Electronic Warfare*,
(Norwood, MA: Artech House Inc, 2001), p 62

⁴⁰ Sergei Vakin, Lev Shustov, Robert Dunwell, *Fundamentals of Electronic Warfare*,
(Norwood, MA: Artech House Inc, 2001), 62

⁴¹ Sergei Vakin, Lev Shustov, Robert Dunwell, *Fundamentals of Electronic Warfare*,
(Norwood, MA: Artech House Inc, 2001), 62-63

⁴² “Russia Delivers GPS Jammer to Counter Missiles”, Doug Richardson, *Jane’s Missiles
& Rockets*, last modified July 30, 2007,
[https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1197
250&Pubabbrev=JMR](https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1197250&Pubabbrev=JMR)

⁴³ “JELS Plans New Frequency Hopping Jammer”, Nick Brown, *International Defence Review*, last modified February 26, 2009,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1106123&Pubabbrev=IDR>

⁴⁴ “SAJ-1030 GPS Jammer”, *Jane’s C4ISR & Mission Systems: Joint & Common Equipment*, last modified February 22, 2012,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1499015&Pubabbrev=JC4IJ>

⁴⁵ “AURA Mobile Communications GPS/WiFi Jammer”, *Jane’s Police and Homeland Security Equipment*, last modified August 29, 2012,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1379747&Pubabbrev=JPSE>

⁴⁶ “Russia Delivers GPS Jammer to Counter Missiles”, Doug Richardson, *Jane’s Missiles & Rockets*, last modified July 30, 2007,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1197250&Pubabbrev=JMR>

⁴⁷ “South Korea Accuses North of GPS Jamming” Sarah McDowall, *Jane’s Defence Weekly*, last modified May 3, 2012,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1506633&Pubabbrev=JDW>

⁴⁸ “Jane’s World Armies: North Korea”, *Jane’s World Armies*, last modified October 18, 2012, <http://www.janes.com/products/janes/security/military-capabilities/world-armies.aspx>

⁴⁹ “South Korea Accuses North of GPS Jamming” Sarah McDowall, *Jane’s Defence Weekly*, last modified May 3, 2012,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1506633&Pubabbrev=JDW>

⁵⁰ “Russia Delivers GPS Jammer to Counter Missiles”, Doug Richardson, *Jane’s Missiles & Rockets*, last modified July 30, 2007,

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1197250&Pubabbrev=JMR>

⁵¹ “GPS Spoofing, Old Threat and New Problems”, Pierluigi Paganini, Security Affairs, last modified February 23, 2012, <http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html>

⁵² “GPS Spoofing, Old Threat and New Problems”, Pierluigi Paganini, Security Affairs, last modified February 23, 2012, <http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html>

⁵³ “GPS Spoofing, Old Threat and New Problems”, Pierluigi Paganini, Security Affairs, last modified February 23, 2012, <http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html>

⁵⁴ Tyler Nighswander , Brent Ledvina , Jonathan Diamond , Robert Brumley, David Brumley, “GPS Software Attacks”, (2012), users.ece.cmu.edu/~dbrumley/courses/18487-f12/.../Nov28_GPS.pdf

⁵⁵ Tyler Nighswander , Brent Ledvina , Jonathan Diamond , Robert Brumley, David Brumley, “GPS Software Attacks”, (2012), users.ece.cmu.edu/~dbrumley/courses/18487-f12/.../Nov28_GPS.pdf

⁵⁶ “Third Testing of China’s Anti-Satellite Weapons?”, The Voice of Russia, last modified January 10, 2013, http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

⁵⁷ “Third Testing of China’s Anti-Satellite Weapons?”, The Voice of Russia, last modified January 10, 2013, http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

⁵⁸ “Third Testing of China’s Anti-Satellite Weapons?”, The Voice of Russia, last modified January 10, 2013, http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

⁵⁹“Third Testing of China’s Anti-Satellite Weapons?”, The Voice of Russia, last modified January 10, 2013, http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

⁶⁰“Third Testing of China’s Anti-Satellite Weapons?”, The Voice of Russia, last modified January 10, 2013, http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

⁶¹“Third Testing of China’s Anti-Satellite Weapons?”, The Voice of Russia, last modified January 10, 2013, http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

⁶² Chief of Naval Operations, Commandant of the Marine Corps, Headquarters United States Coast Guard, “*Universal Naval Task List*”, (Washington, D.C., November 2008) p 4-B-205, <http://www.marines.mil/News/Publications/ELECTRONICLIBRARY/ElectronicLibraryDisplay/tabid/13082/Article/126785/mco-350026a-wch-1-final-corrected-copy.aspx>

⁶³ Dan Lamothe, “Details of Marines’ pilot rescue released”, *Marine Corps Times.com*, March 22, 2011, <http://marinecorpstimes.com/news/2011/03/marine-libya-pilot-rescue-details-released-032211w/>

⁶⁴ Ross Simpson, “The Rescue of Basher 52”, *Marine Corps Gazette*, September 1995, <https://www.mca-marines.org/leatherneck/rescue-basher-52>

⁶⁵ Ross Simpson, “The Rescue of Basher 52”, *Marine Corps Gazette*, September 1995, <https://www.mca-marines.org/leatherneck/rescue-basher-52>

⁶⁶ “AN/PRC-112G CSAR”, General Dynamics C4 Systems, accessed 30 January 2012, <http://www.gdc4s.com/anprc-112g-transceiver.html>

⁶⁷ Dan Lamothe, “Details of Marines’ pilot rescue released”, *Marine Corps Times.com*, March 22, 2011, <http://marinecorpstimes.com/news/2011/03/marine-libya-pilot-rescue-details-released-032211w/>

⁶⁸ “Jane’s World Armies: North Korea”, *Jane’s World Armies*, last modified October 18, 2012, <http://www.janes.com/products/janes/security/military-capabilities/world-armies.aspx>

⁶⁹ Chief of Naval Operations, Commandant of the Marine Corps, Headquarters United States Coast Guard, “*Universal Naval Task List*”, (Washington, D.C., November 2008) p 4-B-I to 4 –B-xvi,
<http://www.marines.mil/News/Publications/ELECTRONICLIBRARY/ElectronicLibraryDisplay/tabid/13082/Article/126785/mco-350026a-wch-1-final-corrected-copy.aspx>

⁷⁰ Congressional Budget Office Study, *The Global Position System for Military Users, Current Modernization Plans and Alternatives*, October 2011, Summary, p 1

⁷¹ “Jane’s World Armies: North Korea”, *Jane’s World Armies*, last modified October 18, 2012, <http://www.janes.com/products/janes/security/military-capabilities/world-armies.aspx>

⁷² Congressional Budget Office Study, *The Global Position System for Military Users, Current Modernization Plans and Alternatives*, October 2011, Summary, p x-xiv

⁷³ Congressional Budget Office Study, *The Global Position System for Military Users, Current Modernization Plans and Alternatives*, October 2011, Summary, p 16

Bibliography

“AN/PRC-112G CSAR.” General Dynamics C4 Systems. <http://www.gdc4s.com/anprc-112g-transceiver.html>

“AURA Mobile Communications GPS/WiFi Jammer.” *Jane's Police and Homeland Security Equipment*. August 29, 2012,
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1379747&Pubabbrev=JPSE>

Brown, Nick. “JELS Plans New Frequency Hopping Jammer.” *International Defence Review*. February 26, 2009.
<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1106123&Pubabbrev=IDR>

Chief of Naval Operations, Commandant of the Marine Corps, Headquarters United States Coast Guard. “*Universal Naval Task List*.” Washington, D.C., November 2008.
<http://www.marines.mil/News/Publications/ELECTRONICLIBRARY/ElectronicLibraryDisplay/tabid/13082/Article/126785/mco-350026a-wch-1-final-corrected-copy.aspx>

Congressional Budget Office Study. *The Global Position System for Military Users, Current Modernization Plans and Alternatives*. October 2011.
www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf

“CSAC Applications.” National Institute of Standards and Technology, Atomic Devices and Instrumentation Group.
http://tf.nist.gov/timefreq/ofm/smallclock/CSAC_Applications.html

Department of Defense. *Annual Report To Congress, Military and Security Developments Involving the People's Republic of China 2011*. Washington, D.C., Office of the Secretary of Defense. May 2011. www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf

Department of Defense. *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*. Washington DC: US Dept of Defense, Sept 2008.
<http://www.gps.gov/technical/ps/>

Department of Defense. *Global Positioning System Standard Positioning Service Performance Standard, 4th Edition*. Washington DC: US Dept of Defense, Sept 2008.

<http://www.gps.gov/technical/ps/>

“GPS.GOV.” National Coordination Officer for Space Based Position, Navigation and Timing (NOAA.) <http://www.gps.gov/>

“Global Positioning System.” GSM Server. <http://www.gsmserver.com/articles/gps.php>

“Jane’s World Armies: North Korea.” *Jane’s World Armies*. October 18, 2012

<http://www.janes.com/products/janes/security/military-capabilities/world-armies.aspx>

Lamothe, Dan. “Details of Marines’ pilot rescue released.” *Marine Corps Times.com*. March 22, 2011. <http://marinecorpstimes.com/news/2011/03/marine-libya-pilot-rescue-details-released-032211w/>

McDowall, Sarah. “South Korea Accuses North of GPS Jamming.” *Jane’s Defence Weekly*. May 3, 2012,

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=++1506633&Pubabbrev=JDW>

Merrill, John. “Patriot Watch VIGILANCE SAFEGUARDING AMERICA.” Powerpoint Presentation, Department of Homeland Security, Position, Navigation & Timing (PNT) Program Management Office. March 2012.

www.gps.gov/multimedia/presentations/2012/03/WSTS/merrill.pdf

Nighswander, Tyler. Brent Ledvina, Jonathan Diamond, Robert Brumley, David Brumley, “GPS Software Attacks.” 2012, users.ece.cmu.edu/~dbrumley/courses/18487-f12/.../Nov28_GPS.pdf

Paganini, Pierluigi. “GPS Spoofing, Old Threat and New Problems.” Security Affairs. February 23, 2012, <http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html>

Richardson, Doug. "Russia Delivers GPS Jammer to Counter Missiles." *Jane's Missiles & Rockets*. July 30, 2007.

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=++1197250&Pubabbrev=JMR>

"SAJ-1030 GPS Jammer," *Jane's C4ISR & Mission Systems: Joint & Common Equipment*. February 22, 2012,

<https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1499015&Pubabbrev=JC4IJ>

Simpson, Ross. "The Rescue of Basher 52." *Marine Corps Gazette*. September 1995.

<https://www.mca-marines.org/leatherneck/rescue-basher-52>

"Third Testing of China's Anti-Satellite Weapons?" *The Voice of Russia*. January 10, 2013.

http://english.ruvr.ru/2013_01_10/Third-testing-of-China-s-anti-satellite-weapons/

U.S. Government. *NAVSTAR GPS User Equipment Introduction*. September 1996.

<http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

Vakin, Sergei. Lev Shustov, Robert Dunwell. *Fundamentals of Electronic Warfare*, Norwood, MA: Artech House Inc, 2001.